Docket No.: 60188-648 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Makoto FUJIWARA, et al.	:	Confirmation Number:
Serial No.:	:	Group Art Unit:
Filed: September 04, 2003	:	Examiner:

For: SEMICONDUCTOR DEVICE INCLUDING ENCRYPTION SECTION, SEMICONDUCTOR DEVICE INCLUDING EXTERNAL INTERFACE, AND CONTENT REPRODUCTION METHOD

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2002-258481, filed September 4, 2002

cited in the Declaration of the present application. A Certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:prg
Facsimile: (202) 756-8087
Date: September 4, 2003

Fujiwara et al.
Sept. 4, 2003
McDermott, Will & Emery

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application: ２００２年 ９月 ４日

出 願 番 号
Application Number: 特願２００２－２５８４８１

[ST.10/C]: [ＪＰ２００２－２５８４８１]

出 願 人
Applicant(s): 松下電器産業株式会社

２００３年 ４月２５日

特 許 庁 長 官
Commissioner,
Japan Patent Office 太田信一郎

出証番号 出証特２００３－３０３０８３０

【書類名】　特許願

【整理番号】　5037540107

【提出日】　平成14年 9月 4日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 15/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　藤原　睦

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　根本　祐輔

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　安井　純一

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　前田　卓治

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　伊藤　孝幸

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　山田　泰司

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　井上　信治

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100077931

【弁理士】

【氏名又は名称】　前田　弘

【選任した代理人】

【識別番号】　100094134

【弁理士】

【氏名又は名称】　小山　廣毅

【選任した代理人】

【識別番号】　100110939

【弁理士】

【氏名又は名称】　竹内　宏

【選任した代理人】

【識別番号】　100110940

【弁理士】

【氏名又は名称】　嶋田　高久

【選任した代理人】

【識別番号】　100113262

【弁理士】

【氏名又は名称】　竹内　祐二

【選任した代理人】

【識別番号】　100115059

【弁理士】

【氏名又は名称】　今江　克実

【選任した代理人】

【識別番号】　100115510

【弁理士】

【氏名又は名称】　手島　勝

【選任した代理人】

【識別番号】　100115691

【弁理士】

【氏名又は名称】　藤田　篤史

【手数料の表示】

【予納台帳番号】　014409

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0006010

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化部を有する半導体装置、外部インターフェースを有する半導体装置、およびコンテンツ再生方法

【特許請求の範囲】

【請求項１】　プログラムの暗号化および復号化のうち少なくともいずれか一方を行う暗号化部を備え、

前記暗号化部は、

プログラムの暗号化処理または復号化処理を含む複数のシーケンスを実行可能な暗号化演算部と、

前記暗号化演算部が実行可能な各シーケンスについて、実行の諾否を判断し、実行が許されないと判断したシーケンスについて、前記暗号化演算部の動作を禁止する暗号化制御部とを備えたものである

ことを特徴とする半導体装置。

【請求項２】　請求項１において、

前記複数のシーケンスは、鍵の暗号化処理または復号化処理を含むものである

ことを特徴とする半導体装置。

【請求項３】　請求項１において、

前記暗号化制御部は、

モードＩＤを格納するためのモードＩＤ格納レジスタを備え、かつ、

前記モードＩＤ格納レジスタに格納されたモードＩＤの値に基づいて、各シーケンスの実行の諾否を判断するものである

ことを特徴とする半導体装置。

【請求項４】　請求項３において、

前記暗号化制御部は、

前記各シーケンスに対応して設けられ、その発行回数を格納するためのレジスタを備え、

前記モードＩＤの値に加えて、前記レジスタに格納された前記各シーケンスの発行回数を加味して、各シーケンスの実行の諾否を判断するものである

ことを特徴とする半導体装置。

【請求項５】　請求項３において、

書き換え不可領域を有するセキュアメモリを備え、前記書き換え不可領域には、前記モードＩＤが記憶されており、

前記モードＩＤ格納レジスタは、当該半導体装置の起動時にのみ書き込み可能であり、かつ、起動時に、前記セキュアメモリの前記書き換え不可領域から読み出された前記モードＩＤが書き込まれる

ことを特徴とする半導体装置。

【請求項６】　請求項５において、

ブートプログラムを記憶するブートＲＯＭを備え、

前記モードＩＤ格納レジスタへの前記モードＩＤの書き込みは、前記ブートＲＯＭに記憶されたブートプログラムによって、実行する

ことを特徴とする半導体装置。

【請求項７】　請求項３において、

当該半導体装置が初めて起動されたか否かを表す実装モードフラグを記憶するセキュアメモリを備え、

前記暗号化制御部は、

前記モードＩＤの値に加えて、前記実装モードフラグを参照して、各シーケンスの実行の諾否を判断するものである

ことを特徴とする半導体装置。

【請求項８】　請求項１において、

前記複数のシーケンスの少なくとも１つについて、これに対応したブートプログラムを記憶するブートＲＯＭを備え、

前記暗号化演算部は、前記ブートＲＯＭに記憶されたブートプログラムを実行することによって、シーケンスを実行するものである

ことを特徴とする半導体装置。

【請求項９】　請求項１において、

前記暗号化演算部および暗号化制御部が有するレジスタについて、当該半導体装置外部からのアクセスができないように制御する手段を備えた

ことを特徴とする半導体装置。

【請求項１０】　外部メモリとの間で、プログラムやデータの入出力を行うための外部インターフェースを備え、

前記外部インターフェースは、

プログラムの入出力を行うプログラム処理部と、

データの入出力を行うデータ処理部とを備え、

前記プログラム処理部と前記データ処理部とは、別個独立に、構成されていることを特徴とする半導体装置。

【請求項１１】　請求項１０において、

前記プログラム処理部は、

プログラムをそのまま入出力するスルー部と、

前記外部メモリに記憶された暗号化プログラムを受け、これを平文プログラムに復号して、当該半導体装置内部に供給するプログラム復号用暗号エンジンとを備えたものである

ことを特徴とする半導体装置。

【請求項１２】　請求項１１において、

前記スルー部は、実行用スルー部と、暗号化用スルー部とを備えており、

前記実行用スルー部を介して入力されたプログラムは、当該半導体装置において実行される一方、前記暗号化用スルー部を介して入力されたプログラムは、暗号化部に供給され、暗号化される

ことを特徴とする半導体装置。

【請求項１３】　請求項１２において、

前記外部メモリにおける各領域と、アドレスとの対応関係を表すアドレス管理情報を格納するアドレス区分格納レジスタを備え、

前記外部メモリにアクセスしてプログラムを読み込むとき、前記アドレス管理情報を参照して、前記暗号化用スルー部、前記実行用スルー部および前記プログラム復号用暗号エンジンのいずれを有効にするかを、決定する

ことを特徴とする半導体装置。

【請求項１４】　請求項１３において、

前記アドレス区分格納レジスタは、当該半導体装置の起動時にのみ書き込み可

能である

ことを特徴とする半導体装置。

【請求項１５】　請求項１４において、

書き換え不可領域を有するセキュアメモリを備え、前記書き換え不可領域には、前記アドレス管理情報が記憶されており、

前記アドレス区分格納レジスタは、当該半導体装置の起動時に、前記セキュアメモリの前記書き換え不可領域から読み出された前記アドレス管理情報が書き込まれる

ことを特徴とする半導体装置。

【請求項１６】　請求項１３において、

モードＩＤを格納するためのモードＩＤ格納レジスタを有するモードシーケンサを備え、

前記モードＩＤ格納レジスタに格納されたモードＩＤの値を加味して、前記暗号化用スルー部、前記実行用スルー部および前記プログラム復号用暗号エンジンのいずれを有効にするかを、決定する

ことを特徴とする半導体装置。

【請求項１７】　請求項１６において、

前記モードシーケンサは、ジャンパ値判定部を備え、

前記ジャンパ値判定部によって判定されたジャンパ値を加味して、前記暗号化用スルー部、前記実行用スルー部および前記プログラム復号用暗号エンジンのいずれを有効にするかを、決定する

ことを特徴とする半導体装置。

【請求項１８】　請求項１０において、

前記データ処理部は、

データをそのまま入出力するスルー部と、

データの入出力の際に、暗号または復号を行うデータ暗復号用暗号エンジンとを備えたものである

ことを特徴とする半導体装置。

【請求項１９】　外部メモリの再生不可領域に格納された原コンテンツを、

ＬＳＩに取り込むステップと、

前記ＬＳＩにおいて、内部メモリに格納された固有ＩＤを用いて、データ固有鍵を生成するステップと、

前記ＬＳＩにおいて、前記原コンテンツを、前記データ固有鍵を用いて暗号化するステップと、

暗号化されたコンテンツを、前記外部メモリの再生可能領域に格納するステップと、

前記再生可能領域に格納された前記暗号化されたコンテンツを、前記ＬＳＩに取り込み、前記データ固有鍵を用いて復号化して再生するステップとを備えたことを特徴とするコンテンツ再生方法。

【請求項２０】　請求項１９において、

前記原コンテンツは、データ共有鍵で暗号化されたものであり、

前記原コンテンツを、前記データ固有鍵を用いて暗号化する前に、内部メモリに格納された前記データ共有鍵を用いて、復号化する

ことを特徴とするコンテンツ再生方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、鍵実装システムに用いられるＬＳＩのような半導体装置において、セキュリティを向上させる技術に属する。

【０００２】

【従来の技術】

本願と同一の出願人による特願２００１－２８６８８１では、鍵実装システムにおいて、鍵の機密性および秘匿性を、従来よりも向上させる技術が示されている。

【０００３】

しかし、かかる先行技術は、文献公知発明に係るものではないため、記載すべき先行技術文献情報はない。

【０００４】

【発明が解決しようとする課題】

本発明は、セキュリティレベルの高い半導体装置を提供することを課題とする。また、セキュリティレベルの高いコンテンツ再生方法を提供することを課題とする。

【０００５】

【課題を解決するための手段】

前記の課題を解決するために、本発明が講じた解決手段は、半導体装置として、プログラムの暗号化および復号化のうち少なくともいずれか一方を行う暗号化部を備え、前記暗号化部は、プログラムの暗号化処理または復号化処理を含む複数のシーケンスを実行可能な暗号化演算部と、前記暗号化演算部が実行可能な各シーケンスについて、実行の諾否を判断し、実行が許されないと判断したシーケンスについて、前記暗号化演算部の動作を禁止する暗号化制御部とを備えたものである。

【０００６】

本発明によると、暗号化部において、暗号化制御部が、暗号化演算部が実行可能な各シーケンスのうち、実行が許されないと判断したシーケンスについて、暗号化演算部の動作を禁止する。すなわち、実行が許されると暗号化制御部によって判断されたシーケンスのみが、暗号化演算部によって実行される。このため、シーケンスの不正実行を未然に防止することができ、セキュリティレベルが向上する。

【０００７】

そして、前記本発明に係る半導体装置における複数のシーケンスは、鍵の暗号化処理または復号化処理を含むのが好ましい。

【０００８】

また、前記本発明に係る半導体装置における暗号化制御部は、モードＩＤを格納するためのモードＩＤ格納レジスタを備え、かつ、前記モードＩＤ格納レジスタに格納されたモードＩＤの値に基づいて、各シーケンスの実行の諾否を判断するのが好ましい。

【０００９】

そして、前記暗号化制御部は、前記各シーケンスに対応して設けられ、その発行回数を格納するためのレジスタを備え、前記モードＩＤの値に加えて、前記レジスタに格納された前記各シーケンスの発行回数を加味して、各シーケンスの実行の諾否を判断するのが好ましい。

【００１０】

また、書き換え不可領域を有するセキュアメモリを備え、前記書き換え不可領域には、前記モードＩＤが記憶されており、前記モードＩＤ格納レジスタは、当該半導体装置の起動時にのみ書き込み可能であり、かつ、起動時に、前記セキュアメモリの前記書き換え不可領域から読み出された前記モードＩＤが書き込まれるのが好ましい。さらに、ブートプログラムを記憶するブートＲＯＭを備え、前記モードＩＤ格納レジスタへの前記モードＩＤの書き込みは、前記ブートＲＯＭに記憶されたブートプログラムによって実行するのが好ましい。

【００１１】

また、当該半導体装置が初めて起動されたか否かを表す実装モードフラグを記憶するセキュアメモリを備え、前記暗号化制御部は、前記モードＩＤの値に加えて、前記実装モードフラグを参照して、各シーケンスの実行の諾否を判断するのが好ましい。

【００１２】

また、前記本発明に係る半導体装置は、前記複数のシーケンスの少なくとも１つについて、これに対応したブートプログラムを記憶するブートＲＯＭを備え、前記暗号化演算部は、前記ブートＲＯＭに記憶されたブートプログラムを実行することによってシーケンスを実行するのが好ましい。

【００１３】

また、前記本発明に係る半導体装置は、前記暗号化演算部および暗号化制御部が有するレジスタについて、当該半導体装置外部からのアクセスができないように制御する手段を備えているのが好ましい。

【００１４】

また、本発明は、半導体装置として、外部メモリとの間で、プログラムやデータの入出力を行うための外部インターフェースを備え、前記外部インターフェー

スは、プログラムの入出力を行うプログラム処理部と、データの入出力を行うデータ処理部とを備え、前記プログラム処理部と前記データ処理部とは、別個独立に、構成されているものである。

【００１５】

本発明によると、外部インターフェースにおいて、プログラム処理部とデータ処理部とが、別個独立に、構成されている。このため、プログラムが不正実行されるリスクが分散されることになり、セキュリティレベルが向上する。

【００１６】

そして、前記本発明に係る半導体装置におけるプログラム処理部は、プログラムをそのまま入出力するスルー部と、前記外部メモリに記憶された暗号化プログラムを受け、これを平文プログラムに復号して、当該半導体装置内部に供給するプログラム復号用暗号エンジンとを備えているのが好ましい。

【００１７】

さらに、前記スルー部は、実行用スルー部と、暗号化用スルー部とを備えており、前記実行用スルー部を介して入力されたプログラムは、当該半導体装置において実行される一方、前記暗号化用スルー部を介して入力されたプログラムは、暗号化部に供給され、暗号化されるのが好ましい。

【００１８】

さらに、前記外部メモリにおける各領域と、アドレスとの対応関係を表すアドレス管理情報を格納するアドレス区分格納レジスタを備え、前記外部メモリにアクセスしてプログラムを読み込むとき、前記アドレス管理情報を参照して、前記暗号化用スルー部、前記実行用スルー部および前記プログラム復号用暗号エンジンのいずれを有効にするかを、決定するのが好ましい。

【００１９】

さらに、前記アドレス区分格納レジスタは、当該半導体装置の起動時にのみ書き込み可能であるのが好ましい。

【００２０】

さらに、書き換え不可領域を有するセキュアメモリを備え、前記書き換え不可領域には、前記アドレス管理情報が記憶されており、前記アドレス区分格納レジ

スタは、当該半導体装置の起動時に、前記セキュアメモリの前記書き換え不可領域から読み出された前記アドレス管理情報が書き込まれるのが好ましい。

【００２１】

または、モードＩＤを格納するためのモードＩＤ格納レジスタを有するモードシーケンサを備え、前記モードＩＤ格納レジスタに格納されたモードＩＤの値を加味して、前記暗号化用スルー部、前記実行用スルー部および前記プログラム復号用暗号エンジンのいずれを有効にするかを、決定するのが好ましい。

【００２２】

さらに、前記モードシーケンサは、ジャンパ値判定部を備え、前記ジャンパ値判定部によって判定されたジャンパ値を加味して、前記暗号化用スルー部、前記実行用スルー部および前記プログラム復号用暗号エンジンのいずれを有効にするかを決定するのが好ましい。

【００２３】

また、前記本発明に係る半導体装置におけるデータ処理部は、データをそのまま入出力するスルー部と、データの入出力の際に、暗号または復号を行うデータ暗復号用暗号エンジンとを備えているのが好ましい。

【００２４】

また、本発明が講じた解決手段は、コンテンツ再生方法として、外部メモリの再生不可領域に格納された原コンテンツをＬＳＩに取り込むステップと、前記ＬＳＩにおいて、内部メモリに格納された固有ＩＤを用いて、データ固有鍵を生成するステップと、前記ＬＳＩにおいて、前記原コンテンツを、前記データ固有鍵を用いて暗号化するステップと、暗号化されたコンテンツを、前記外部メモリの再生可能領域に格納するステップと、前記再生可能領域に格納された前記暗号化されたコンテンツを、前記ＬＳＩに取り込み、前記データ固有鍵を用いて復号化して再生するステップとを備えたものである。

【００２５】

本発明によると、外部メモリの再生不可領域に格納された原コンテンツは、ＬＳＩにおいて、内部メモリに格納された固有ＩＤを用いて生成されたデータ固有鍵を用いて、暗号化される。暗号化されたコンテンツは、外部メモリの再生可能

領域に格納され、再生のとき、データ固有鍵を用いて復号化される。このため、外部メモリの再生可能領域には、固有ＩＤから生成されたデータ固有鍵を用いて暗号化されたコンテンツが格納されるので、同一のデータ固有鍵を有しない他のＬＳＩによっては、再生が不能となる。このため、コンテンツの不正実行が防止され、セキュリティレベルが向上する。

【００２６】

そして、前記本発明に係るコンテンツ再生方法において、前記原コンテンツは、データ共有鍵で暗号化されたものであり、前記原コンテンツを、前記データ固有鍵を用いて暗号化する前に、内部メモリに格納された前記データ共有鍵を用いて、復号化するのが好ましい。

【００２７】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照して説明する。

【００２８】

図１は本実施形態に係る半導体装置としてのセキュアＬＳＩの内部構成を示すブロック図である。図１において、セキュアＬＳＩ１は外部バス１２０を介して、外部メモリ１００（フラッシュメモリ１０１とＲＡＭ１０２）などと接続可能に構成されている。また、モードＩＤを与えることによって、その動作モードを設定することが可能になっている。

【００２９】

本実施形態に関わる主な構成要素について、簡単に説明する。

【００３０】

まず、セキュアＬＳＩ１は、書き換え不可領域１１を含むセキュアメモリ（セキュアＦｌａｓｈ）１０を備えている。この書き換え不可領域１１には、書き換え不可領域書き込みフラグ１２が設けられている。書き換え不可領域書き込みフラグ１２は、モードＩＤが一度セキュアメモリ１０に書き込まれると、そのフラグ値が“可”から“済”になり、それ以降の書き換え不可領域１１への書き込みを不能にする。なお、本実施形態では、セキュアメモリ１０はフラッシュメモリによって構成されているが、もちろんこれに限定されるものではなく、不揮発性

のメモリであればどのようなものであってもかまわない。

【００３１】

また、暗号化部２はプログラムの暗号化や復号化を行うものであり、暗号化演算部としての秘密鍵演算処理部２０と、暗号化制御部としての鍵生成・更新シーケンサ３０と、プログラム暗号種を記憶する記憶部３５とを備えている。秘密鍵演算処理部２０は各種の鍵などを格納するレジスタを備えており、プログラムの暗号化処理または復号化処理を含む複数のシーケンスを実行可能である。鍵生成・更新シーケンサ３０は秘密鍵演算処理部２０が実行可能な各シーケンスについて実行の諾否を判断し、実行が許されないと判断したシーケンスについて秘密鍵演算処理部２０の動作を禁止する。鍵生成・更新シーケンサ３０はモードＩＤ格納レジスタ３１を有しており、このモードＩＤ格納レジスタ３１に格納されているモードＩＤの値に基づいて、各シーケンスの実行の諾否を判断する。また、鍵またはプログラムがどのようなアルゴリズムや鍵長で暗号化されているかを示す暗号種別識別子を格納する暗号種別識別子格納レジスタ３２を備えている。暗号化部２の構成および動作の詳細については、後述する。

【００３２】

モードシーケンサ４０も、モードＩＤ格納レジスタ４１を備えており、モードＩＤ格納レジスタ４１に格納されているモードＩＤと、ジャンパ４３の値に応じて、外部インターフェース（Ｉ／Ｆ）５０の動作、すなわち、外部メモリ１００に格納されたプログラムやデータをどのＩ／Ｆを介して読み込むか、が制御される。これにより、外部メモリ１００に格納された平文プログラムが実行できるか否かを制御することができる。さらに、モードシーケンサ４０は、鍵がどの手法によって暗号化されているかを示す暗号種別識別子を格納する暗号種別識別子格納レジスタ４２を備えている。

【００３３】

外部Ｉ／Ｆ５０は、モードシーケンサ４０の制御に従って、プログラム処理部５１が有するスルー部５２およびプログラム復号用暗号エンジン５３、並びに、データ処理部５５が有するスルー部５６およびデータ暗復号用暗号エンジン５８のうちのいずれかを介して、外部メモリ１００との間でプログラムやデータの入

出力を行う。

【００３４】

ここで、後述するアドミニストレータモードとアプリプログラム開発を除いては、スルー部５２を介して入力されたプログラムは、セキュアＬＳＩ１内部で実行されることはない。すなわち、スルー部５２は、平文プログラムの暗号化、またはすでに暗号化されたプログラムを別の鍵を用いて再暗号化するときに有効とされるものであり、セキュアＬＳＩ１は、後述するアドミニストレータモードとアプリプログラム開発を除いては、スルー部５２を介して入力されたプログラムへは動作を遷移しないように構成されている。したがって、例えば商品となったセキュアＬＳＩ１はスルー部５２を介して平文プログラムを取り込んだとしても、これを実行することはできない。

【００３５】

ブートＲＯＭ６０は、セキュアＬＳＩ１の起動動作を制御するブートプログラムを格納している。ＨＡＳＨ演算部７０は、セキュアＬＳＩ１に読み込まれたプログラムについてその正当性を検証するために、ＨＡＳＨ値を演算する。

【００３６】

また、外部メモリ１００では、プログラムがフラッシュメモリ１０１に格納され、データ（コンテンツ）がＲＡＭ１０２に格納されている。外部ツール１１０には、セキュアＬＳＩ１の最初の起動時にセキュアメモリ１０に格納する各種の初期値が格納されている。この初期値の種類は、設定される動作モードに応じて、異なったものになる。

【００３７】

図２は図１のセキュアＬＳＩ１を用いた開発および製品化の全体の流れを表す図である。図２に示すように、セキュアＬＳＩ１は、アドミニストレータモード（モードＩＤ：００）、鍵生成モード（モードＩＤ：０１）、開発モード（モードＩＤ：１０）および商品動作モード（モードＩＤ：１１）の４種類の動作モードで、動作する。

【００３８】

まず、アドミニストレータモードに設定されたセキュアＬＳＩ１は、管理者用

ＬＳＩとして、動作する。管理者用ＬＳＩでは、鍵生成プログラムが開発され（ＰＡ１）、また、その鍵生成プログラムが任意の鍵生成鍵を用いて暗号化される（ＰＡ２）。

【００３９】

鍵生成モードに設定されたセキュアＬＳＩ１は、鍵生成用ＬＳＩとして、動作する。鍵生成用ＬＳＩでは、管理者用ＬＳＩにおいて生成された、暗号化された鍵生成プログラムが実装され（ＰＢ１）、この鍵生成プログラムを実行することによって、各種の鍵が生成される（ＰＢ２）。

【００４０】

開発モードに設定されたセキュアＬＳＩ１は、開発用ＬＳＩとして、動作する。開発用ＬＳＩでは、実際の製品で実行されるアプリケーション用プログラムが開発される（ＰＣ１）。そして、このアプリケーション用プログラムが、プログラム共有鍵を用いて暗号化される（ＰＣ２）。

【００４１】

商品動作モードに設定されたセキュアＬＳＩ１は、実際の商品ＬＳＩとして、動作する。商品ＬＳＩでは、開発用ＬＳＩにおいて生成された、プログラム共有鍵で暗号化されたアプリケーション用プログラムが実装され、その内部で、プログラム固有鍵で暗号化されたアプリケーション用プログラムに、変換される（ＰＤ１）。プログラム固有鍵で暗号化されたアプリケーションプログラムは通常の商品動作において実行される。なお、この変換処理は、開発用ＬＳＩでも、アプリケーション用プログラムのデバッグ（ＰＣ４）のために、実行可能になっている（ＰＣ３）。

【００４２】

セキュアＬＳＩ１は、ブートＲＯＭ６０に格納されたブートプログラムを実行することによって、以下のような動作を行う。

【００４３】

図３はブートプログラムの全体的な処理の流れを示すフローチャートである。セキュアＬＳＩ１に電源が投入されると、ブートＲＯＭ６０に格納されたブートプログラムがＣＰＵ６５によって実行される。図３に示すように、まず、各ハー

ドウェアを初期化する（ＳＺ０）。そして、外部ツール１１０からさまざまな初期値を読み込み、セキュアメモリ１０に設定する（ＳＺ１）。

【００４４】

図４は初期値設定処理ＳＺ１のフローチャートである。まず、ジャンパ４４で、セキュアメモリ１０がＬＳＩ内に実装されているか否かの判定を行う（ＳＺ１１）。次に、書き換え不可領域書き込みフラグ１２が“済”であるか否かを判定し（ＳＺ１２）、“済”であるときは（ＳＺ１２でＹｅｓ）すでにセキュアメモリ１０に初期値が設定されているので、処理ＳＺ１を終了する。書き換え不可領域書き込みフラグ１２が“可”であるときは（ＳＺ１２でＮｏ）、セキュアメモリ１０に初期値を書き込んでいく。モードＩＤに加えて、暗号化されたプログラム固有鍵、アドレス管理情報、データ固有鍵をセキュアメモリ１０の書き換え不可領域１１に書き込む（ＳＺ１３，ＳＺ１６～ＳＺ１８）。なお、最初の判定の結果、セキュアメモリ１０がＬＳＩの外部にあると判定されたとき（ＳＺ１４でＮｏ）は、モードＩＤは商品動作モードを表す値に上書きされる（ＳＺ１５）。これにより、セキュアメモリ１０がＬＳＩパッケージ外にあるような製品は、商品動作モードでしか動作できない。

【００４５】

次に、書き込み不可領域書き込みフラグ１２を“済”にセットする（ＳＺ１９）。これによって、以後の書き換え不可領域１１の書き換えはできなくなる。さらに、通常領域１３，１４に暗号種別識別子および実装モードフラグを書き込む（ＳＺ１Ａ）。そして、モードＩＤがアドミニストレータモード以外のモードを示すときは（ＳＺ１ＢでＮｏ）、これらに加えて、暗号化された共有鍵／鍵生成鍵も通常領域１３，１４に書き込む（ＳＺ１Ｃ）。

【００４６】

その後、図３にもどり、前処理ＳＺ２を実行する。ここでは、セキュアメモリ１０の書き込み不可領域１１に設定されたモードＩＤが、鍵生成・更新シーケンサ３０のモードＩＤ格納レジスタ３１と、モードシーケンサ４０のモードＩＤ格納レジスタ４１とに設定される。また、セキュアメモリ１０の第１の通常領域１３に設定された暗号種別識別子が、鍵生成・更新シーケンサ３０の暗号種別識別

子格納レジスタ３２と、モードシーケンサ４０の暗号種別識別子格納レジスタ４２とに設定される。さらに、セキュアメモリ１０の書き換え不可領域１１に格納されたアドレス管理情報が、ＭＥＭＣ８０のアドレス区分格納レジスタ８１に設定される。ここまでの動作は、図２における初期値設定フェーズＰＡ０，ＰＢ０，ＰＣ０，ＰＤ０に対応している。

【００４７】

その後は、モードＩＤの値に応じて、それぞれのモードにおける動作を行う（ＳＺ３）。

【００４８】

モードＩＤが「００」のとき、セキュアＬＳＩ１はアドミニストレータモードになり、ジャンパ４３の値に応じて（ＳＡ０）、平文プログラム実行処理ＳＡ１、またはプログラム暗号化処理ＳＡ２を実行する。鍵生成プログラム開発フェーズＰＡ１では、平文プログラム実行処理ＳＡ１が行われ、ここで、鍵生成プログラムが生成される。この鍵生成プログラムは外部メモリ１００に格納される。鍵生成プログラム暗号化フェーズＰＡ２では、鍵生成プログラムを任意の鍵生成鍵で暗号化する。

【００４９】

モードＩＤが「０１」のとき、セキュアＬＳＩ１は鍵生成モードになり、実装モードフラグの値に応じて（ＳＢ０）、キージェネレータ製造処理ＳＢ１、または鍵管理・発行処理ＳＢ２を実行する。キージェネレータ製造フェーズＰＢ１では、キージェネレータ製造処理ＳＢ１が実行され、任意の鍵生成鍵で暗号化された鍵生成プログラムをプログラム固有鍵で再暗号化する。鍵管理・発行フェーズＰＢ２では、プログラム固有鍵で暗号化された鍵生成プログラムを実行させることによって、鍵管理・発行処理ＳＢ２が実行し、鍵を生成する。

【００５０】

モードＩＤが「１０」のとき、セキュアＬＳＩ１は開発モードになり、ジャンパ４３の値に応じて（ＳＣ０）、プログラム暗号化処理ＳＣ１、平文プログラム実行処理ＳＣ２、プログラム実装処理ＳＣ３、または暗号化プログラム実行処理ＳＣ４を実行する。アプリケーションプログラム開発フェーズＰＣ１では、平文

プログラム実行処理ＳＣ２が行われ、アプリケーションプログラムが開発される。開発されたアプリケーションプログラムは、外部メモリ１００に格納される。アプリケーションプログラム暗号化フェーズＰＣ２では、プログラム暗号化処理ＳＣ１が実行される。また、アプリケーションプログラム実装フェーズＰＣ３では、プログラム実装処理ＳＣ３が実行され、アプリケーションプログラムデバッグフェーズＰＣ４では、暗号化プログラム実行処理ＳＣ４が実行される。これらの処理は、商品動作モードにおける各処理ＳＤ１，ＳＤ２と同様である

モードＩＤが「１１」のとき、セキュアＬＳＩ１は商品動作モードになり、実装モードフラグの値に応じて（ＳＤ０）、プログラム実装処理ＳＤ１、または通常ブート処理ＳＤ２を実行する。商品実装フェーズＰＤ１では、プログラム実装処理ＳＤ１が実行される。商品動作フェーズＰＤ２では、通常ブート処理ＳＤ２が実行される。

【００５１】

図５は暗号化部２とその周辺の構成を示す図である。図５に示すように、鍵生成・更新シーケンサ３０はモードＩＤ格納レジスタ３１および暗号種別識別子格納レジスタ３２の他に、秘密演算処理部２０を用いて実行される各シーケンスに対応して設けられ、その発行回数を格納するためのレジスタ３３と、レジスタ３１，３３を参照して、各シーケンスを実行してよいか否か（ブートＲＯＭ６０中の各プログラムおよび外部のプログラムを実行してよいか否か）を判断し、秘密鍵演算処理部２０の動作を制御する制御部３４とを備えている。セキュアＬＳＩ１において、各シーケンスが１回発行されると、これに対応したレジスタ３３に１が加算される。

【００５２】

プログラム暗号種３５は、鍵を復号するとき、または鍵を生成するときに用いられるものであり、共有鍵用と固有鍵用とがそれぞれ準備されている。

【００５３】

そして、上述の商品動作モードや開発モードにおいては、セキュアメモリ１０に格納された値を暗号化部２の各レジスタに設定するシーケンス（セキュアＦｌａｓｈローダー）や鍵を生成・復号するシーケンス（鍵シーケンサ）はそれぞれ

１回ずつしか発行できないように、制御部３４によって制限がかけられる。例えば、セキュアＬＳＩ１の起動時に一度、ブートプログラムによってセキュアメモリに記憶されたモードＩＤがモードＩＤ格納レジスタ３１に格納されると、二度とモードＩＤを書き換えることができない。また、セキュアＬＳＩ起動時に共有鍵と固有鍵を復号し、秘密鍵演算処理部２０内部のレジスタに格納すると、二度と鍵を生成・復号することはできない。したがって、外部メモリ１００に鍵生成プログラムを実装したとしても、鍵は生成することはできない。一度復号された固有鍵は、外部Ｉ／Ｆ５０内の固有鍵格納レジスタに格納され、暗号化プログラムの実行はこの固有鍵を用いて行われる。また、プログラムの更新は、秘密鍵演算処理部２０内部のレジスタに格納された共有鍵や固有鍵を用いて行われる。

【００５４】

なお、上述の鍵生成モードやアドミニストレータモードにおいては、鍵シーケンサに対する制限が外されるので、鍵を生成することができる。

【００５５】

ここで、シーケンス発行回数格納レジスタ３３の代わりに、プログラム暗号種に対応して設けられ、その使用回数を格納するプログラム暗号種使用回数格納レジスタを設けてもよい。鍵を生成・復号するときにはプログラム暗号種が用いられるので、例えば、モードＩＤによってその使用回数を制限しておけば、プログラム暗号種の使用回数を計数することによっても、鍵の生成・復号を制限することができる。

【００５６】

また、プログラム暗号種は必ずしも共有鍵と固有鍵とをそれぞれ準備する必要はない。

【００５７】

図６はコモンバスとプライベートバスの設定方法を示す図である。ここで、「プライベートバス」とは、外部からのアクセス（外部アクセス）ができないバスのことをいい、外部Ｉ／Ｆ５０から必ずしも物理的に独立しているわけではない。すなわち、プライベートバス９１につながっているとして設定されたレジスタ等は、外部アクセスでの読み出し・書き込みができない。

【００５８】

セキュアＬＳＩ１の内部のレジスタ等には、アドレスがそれぞれ与えられている。コモンバスアドレス格納部８２はそのアドレスのうち、コモンバス９２につながったレジスタ等のアドレス（図６では“０Ｘ０００００”～“０Ｘ１００００”）を記憶している。外部アクセスがあったときは、外部アクセスアドレス判定部８３が、コモンバスアドレス格納部８２を参照してコモンバス９２へのアクセスか否かを判定し、そうであればこれを受け付ける。一方、外部アクセスがコモンバス９２へのアクセスでないときは、プライベートバス９１へのアクセスであるので、アクセスを拒否する。

【００５９】

なお、ＣＰＵ６５からのアクセス（内部アクセス）のときは、このような判定は行われず、内部アクセスは受け付けられる。

【００６０】

図７は外部Ｉ／Ｆ５０とその周辺の構成を示す図である。図７において、アドレス区分格納レジスタ８１は、外部メモリ１００における各領域と、アドレスとの対応関係を表すアドレス管理情報を格納している。ここでは、外部メモリ１００を、第１の領域（設定範囲内のプログラム）、第２の領域（設定範囲外のプログラム）、第３の領域（設定範囲内のデータ）および第４の領域（設定範囲外のデータ）という４つの領域に分けて、そのアドレスを記憶している。

【００６１】

比較器８５は、アドレス区分格納レジスタ８１に格納されたアドレス管理情報を参照し、入出力しようとする情報のアドレスが上述の第１～第４の領域のいずれに該当するかを判断し、その判断結果を入出力制御信号生成部８４に送る。

【００６２】

入出力制御信号生成部８４は、モードシーケンサ４０から出力されたモードＩＤとジャンパ判定結果、および比較器８５の出力に基づいて、外部Ｉ／Ｆ５０が有するどのインターフェースを有効にするかを判定し、その判定結果を入出力制御信号として外部入出力モード制御部５４に送る。外部入出力モード制御部５４は受けた入出力制御信号に従って、いずれかのインターフェースを有効にする。

なお、モードＩＤが商品動作モードを示すときは、実行スルー部５２ｂは必ず有効にはしない。これにより、外部メモリ１００に格納された平文プログラムは実行されないように制限される。

【００６３】

第１の領域に格納されたプログラムは、アドミニストレータモードや開発モードのデバッグ時は、プログラム処理部５１の実行用スルー部５２ｂを介して取り込まれ、鍵生成モード、商品動作モード、または開発モードでデバッグ時以外のときは、プログラム復号用暗号エンジン５３を介して取り込まれる。これらのプログラムは実行可能である。一方、第２の領域に格納されたプログラムは、プログラム処理部５１の暗号化用スルー部５２ａを介して取り込まれ、暗号化部２に供給され、暗号化または再暗号化される。これらのプログラムは実行不可能である。

【００６４】

また、第３の領域に格納されたデータは、データ処理部５５のデータ暗復号用暗号エンジン５８を介して取り込まれ、第４の領域に格納されたデータは、データ処理部５５のスルー部５６を介して取り込まれる。

【００６５】

暗号化用スルー部５２ａを介して取り込まれたプログラムは、暗号化部２の秘密鍵演算処理部２０において暗号化または再暗号化された後、再び暗号化スルー部５２ａを介して、外部メモリ１００の第１の領域に書き込まれる。これにより、以降は実行可能なプログラムとなる。

【００６６】

なお、アドレス区分格納レジスタ８１およびモードＩＤ格納レジスタ４１は、プライベートバス９１を介して、データが設定される。すなわち、内部からのアクセスによってデータ設定がなされる。また、このデータ設定は、セキュアＬＳＩ１のリセット後、１回のみ実行可能である。

【００６７】

図８は外部Ｉ／Ｆ５０の動作を示す図であり、商品動作モードを想定している。図８に示すとおり、実装前には、共有鍵で暗号化されたアプリケーションプロ

グラムが外部メモリ１００の第２の領域（設定範囲外）に格納されており、このため、このままでは実行することができない。すなわち、第２の領域に格納された，共有鍵で暗号化されたアプリケーションプログラムは、実装時に暗号化用スルー部５２ａを介してセキュアＬＳＩ１内部に取り込まれ、共有鍵で復号化された後、固有鍵で再暗号化され、再び暗号化用スルー部５２ａを介して、外部メモリ１００の第１の領域（設定範囲内）に格納される。そして、この第１の領域に格納された，固有鍵で暗号化されたアプリケーションプログラムは、プログラム復号用暗号エンジン５３を介してセキュアＬＳＩ１内部に取り込まれ、実行される。

【００６８】

なお、開発モードでは、次のような動作を行う。まずデバッグ時には、実行したいプログラムを第１の領域（設定範囲内）に書き込んでおく。これにより、平文プログラムであっても、実行用スルー部５２ｂを介して取り込まれ、実行される。暗号化時には、暗号化したいプログラムを第２の領域（設定範囲外）に書き込んでおく。これにより、セキュアＬＳＩ１を起動すると、暗号化シーケンスが実行され、共有鍵で暗号化されて外部メモリ１００に格納される。デバッグ実装時には、再暗号化したいプログラムを第２の領域（設定範囲外）に書き込んでおく。さらには、暗号化デバッグ時には、デバッグしたい暗号化プログラムを第１の領域（設定範囲内）に書き込んでおく。これにより、復号されて実行される。

【００６９】

図９はセキュアメモリ１０のアクセス制御を示す図である。図９に示すように、アクセス制御部９５は、書き換え不可領域１１のアドレスを格納するレジスタ９６と、書き換え不可領域書き込みフラグ１２のアドレスを記憶するレジスタ９７と、書き込み可／不可判定部９８とを備えている。レジスタ９６，９７は、データが一度書き込まれると、フラグ管理などによって、さらなる書き込みができないように構成されている。

【００７０】

アクセス制御は、次のように行われる。ＣＰＵ６５からセキュアメモリ１０へのアクセスは、必ず、アクセス制御部９５を介して実行される。コマンドが「リ

ード」のときは、アクセス先のアドレスが、書き換え不可領域または通常領域のいずれであっても、セキュアメモリ１０のデータはプライベートバス９１に出力される。一方、コマンドが「ライト」のときは、書き込み可／不可判定部９８が、アクセス先のアドレスとレジスタ９６に格納されたアドレス、および書き換え不可領域書き込みフラグ１２の値を参照して、書き込みを行うか否かを判定する。具体的には、次のような判断を行う。

（フラグ“済”　かつ　書き込み不可領域）…　書き込み不可
（フラグ“済”　かつ　通常領域）　　…　書き込み可
（フラグ“未”　かつ　書き込み不可領域）…　書き込み可
（フラグ“未”　かつ　通常領域）　　…　書き込み可

【００７１】

なお、セキュアメモリ１０には、「セクタ消去」や「チップ消去」などのコマンドも準備されている。書き換え不可領域書き込みフラグ１２が“済”のとき、「セクタ消去」は通常領域については受け付けるが、書き込み不可領域については受け付けない。また「チップ消去」は受け付けない。

【００７２】

また、コンテンツ（データ）の再生においても、次のような方法を採用することによって、セキュリティを向上させている。

【００７３】

データは当初、外部ＲＡＭ１０２における第４の領域（設定範囲外）に置かれている。第４の領域に置かれているとき、データは、データ共有鍵（プログラム共有鍵と異なる）によって暗号化された状態か、または平文の状態である。このため、他のＬＳＩによって不正利用される可能性があり、セキュリティの面で問題がある。

【００７４】

この問題を解決するために、不正利用を特に防止したい映像や音楽等のコンテンツについては、コンテンツを再生するプログラムを、外部ＲＡＭ１０２の第３の領域（設定範囲内）に記憶されたコンテンツしか再生できないように作成する。第３の領域内に置かれたデータは、セキュアＬＳＩに取り込まれるとき、デー

タ暗復号用暗号エンジン５８において復号化される。この復号化において用いられるデータ固有鍵は、固有ＩＤと乱数によって作成されるので、セキュアＬＳＩ１毎に異なるだけでなく、起動毎にも異なっている。したがって、データは不正利用されにくくなり、セキュリティが向上する。なお、コンテンツを再生するプログラムも固有鍵で暗号化されているので、改竄されにくいと考えられる。

【００７５】

図１０および図１１は商品動作モードにおける通常ブート処理のデータフローである。図１０において、まず、セキュアメモリ１０の書き込み不可領域１１に格納されている、暗号化されたプログラム固有鍵Ｅｎｃ（プログラム固有鍵、ＭＫ０），Ｅｎｃ（ＭＫ０，ＣＫ）を秘密鍵演算処理部２０の暗号鍵格納レジスタに設定する。そして、この暗号化されたプログラム固有鍵を、実装されたプログラム暗号種を用いて復号し、プログラム固有鍵を得る。得たプログラム固有鍵は、外部Ｉ／Ｆ５０のプログラム復号用暗号エンジン５３のプログラム固有鍵格納レジスタに設定する。その後、セキュアメモリ１０の書き込み不可領域１１に格納されているデータ固有ＩＤを秘密鍵演算処理部２０の固有ＩＤ格納レジスタに設定する。また、ＣＰＵ６５によって乱数を生成し、秘密鍵演算処理部２０の乱数格納レジスタに設定する。そして、秘密鍵演算処理部２０によって、データ固有ＩＤと乱数からデータ固有鍵を生成する。生成されたデータ固有鍵は、外部Ｉ／Ｆ５０のデータ暗復号用暗号エンジン５８のデータ固有鍵格納レジスタに設定される。

【００７６】

その後、図１１において、外部メモリ１００に格納されていた，プログラム固有鍵で暗号化されたアプリケーションプログラムＥｎｃ（アプリケーションプログラム，プログラム固有鍵）を、外部Ｉ／Ｆ５０が有するプログラム処理部５１のプログラム復号用暗号エンジン５４を介して復号し、ＨＡＳＨ演算部７０に取り込み、ＨＡＳＨ値を演算する。そして、この演算したＨＡＳＨ値と、セキュアメモリ１０の通常領域１３に格納されていたＨＡＳＨ値とを比較し、アプリケーションプログラムが改ざんされていないかどうかをチェックする。ＨＡＳＨ値が一致していたとき、外部メモリ１００に格納されていたアプリケーションプログ

ラムＥｎｃ（アプリケーションプログラム，プログラム固有鍵）に処理を遷移し、アプリケーションを実行する。なお、ＨＡＳＨ値が一致していないときは、何らかの不正が行われたものと推定して、不正アクセス時制御による処理を実行する。

【００７７】

アプリケーションプログラムは、ＣＰＵ６５によって実行される。すなわち、セキュアＬＳＩ１内部のＣＰＵ６５がマスターとなってアクセス制御を行うので、以降の動作は内部アクセスとなり、したがって、外部アクセスアドレス判定部８３は関与しない。アプリケーションプログラムによって、外部ＲＡＭ１０２の第４の領域（再生不可領域）から、データ共有鍵で暗号化されたコンテンツ（原コンテンツ）がセキュアＬＳＩ１に取り込まれる。取り込まれたコンテンツは、セキュアメモリ１０に書き込まれたデータ共有鍵を用いて、秘密鍵演算処理部２０において復号化される。その後、外部Ｉ／Ｆ５０のデータ処理部５５におけるデータ暗復号用暗号エンジン５８を介してデータ固有鍵で暗号化され、外部ＲＡＭ１０２の第３の領域（再生可能領域）に書き込まれる。以降、このデータ固有鍵で暗号化されたコンテンツは再生可能となり、再生されるとき、外部Ｉ／Ｆ５０のデータ処理部５５におけるデータ暗復号用暗号エンジン５８を介して、データ固有鍵で復号化される。

【００７８】

【発明の効果】

以上のように本発明によると、実行が許されると暗号化制御部によって判断されたシーケンスのみが、暗号化演算部によって実行される。このため、シーケンスの不正実行を未然に防止することができる。また外部インターフェースにおいて、プログラム処理部とデータ処理部とが別個独立に構成されている。このため、プログラムが不正実行されるリスクが分散される。さらに、外部メモリの再生可能領域には、固有ＩＤから生成されたデータ固有鍵を用いて暗号化されたコンテンツが格納されるので、同一のデータ固有鍵を有しない他のＬＳＩによっては再生が不能となる。このため、コンテンツの不正実行が防止される。したがって、セキュリティレベルが向上する。

【図面の簡単な説明】

【図１】

本発明の実施形態に係る半導体装置としてのセキュアＬＳＩの構成を示すブロック図である。

【図２】

図１のセキュアＬＳＩを用いた開発および製品化の全体の流れを表す図である。

【図３】

ブートプログラムの全体的な処理の流れを示すフローチャートである。

【図４】

初期値設定処理ＳＺ１のフローチャートである。

【図５】

図１のセキュアＬＳＩにおける暗号化部とその周辺の構成を示す図である。

【図６】

図１のセキュアＬＳＩにおけるコモンバスとプライベートバスの設定方法を示す図である。

【図７】

図１のセキュアＬＳＩにおける外部ホストＩ／Ｆとその周辺の構成を示す図である。

【図８】

商品動作モードにおける外部ホストＩ／Ｆの動作を示す図である。

【図９】

セキュアメモリのアクセス制御を示す図である。

【図１０】

商品動作モードにおける通常ブート処理のデータフローその１である。

【図１１】

商品動作モードにおける通常ブート処理のデータフローその２である。

【符号の説明】

１　セキュアＬＳＩ（半導体装置）

２　暗号化部

１０　セキュアメモリ

１１　書き換え不可領域

２０　秘密鍵演算処理部（暗号化演算部）

３０　鍵生成・更新シーケンサ（暗号化制御部）

３１　モードＩＤ格納レジスタ

３３　シーケンス発行回数格納レジスタ

３５　記憶部

４０　モードシーケンサ

４１　モードＩＤ格納レジスタ

４５　ジャンパ値判定部

５０　外部インターフェース

５１　プログラム処理部

５２　スルー部

５２ａ　実行用スルー部

５２ｂ　暗号化用スルー部

５３　プログラム復号用暗号エンジン

５５　データ処理部

５６　スルー部

５８　データ暗復号用暗号エンジン

６０　ブートＲＯＭ

８１　アドレス区分格納レジスタ

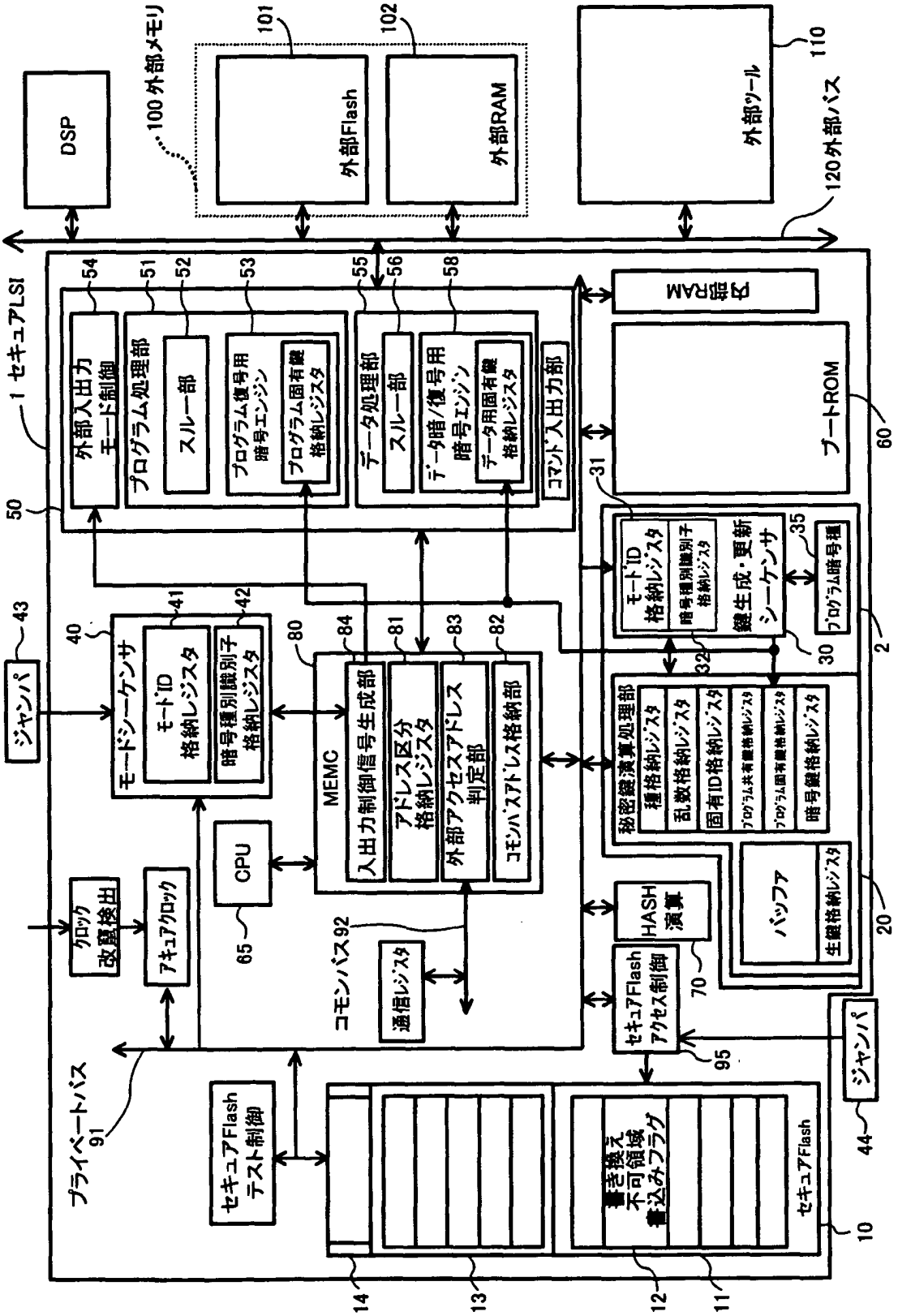
８２　コモンバスアドレス格納部

８３　外部アクセスアドレス判定部

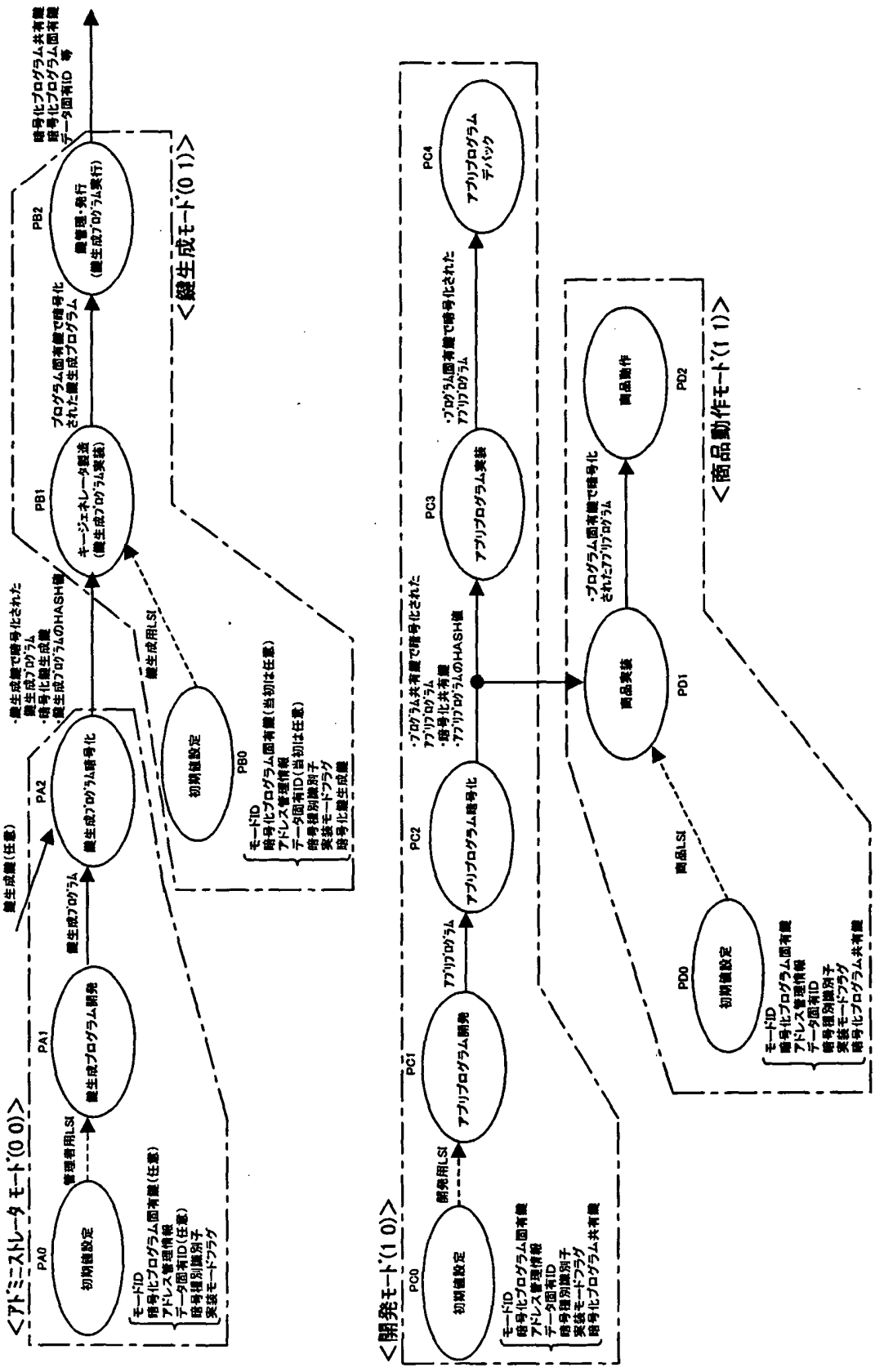
１００　外部メモリ

【書類名】　図面

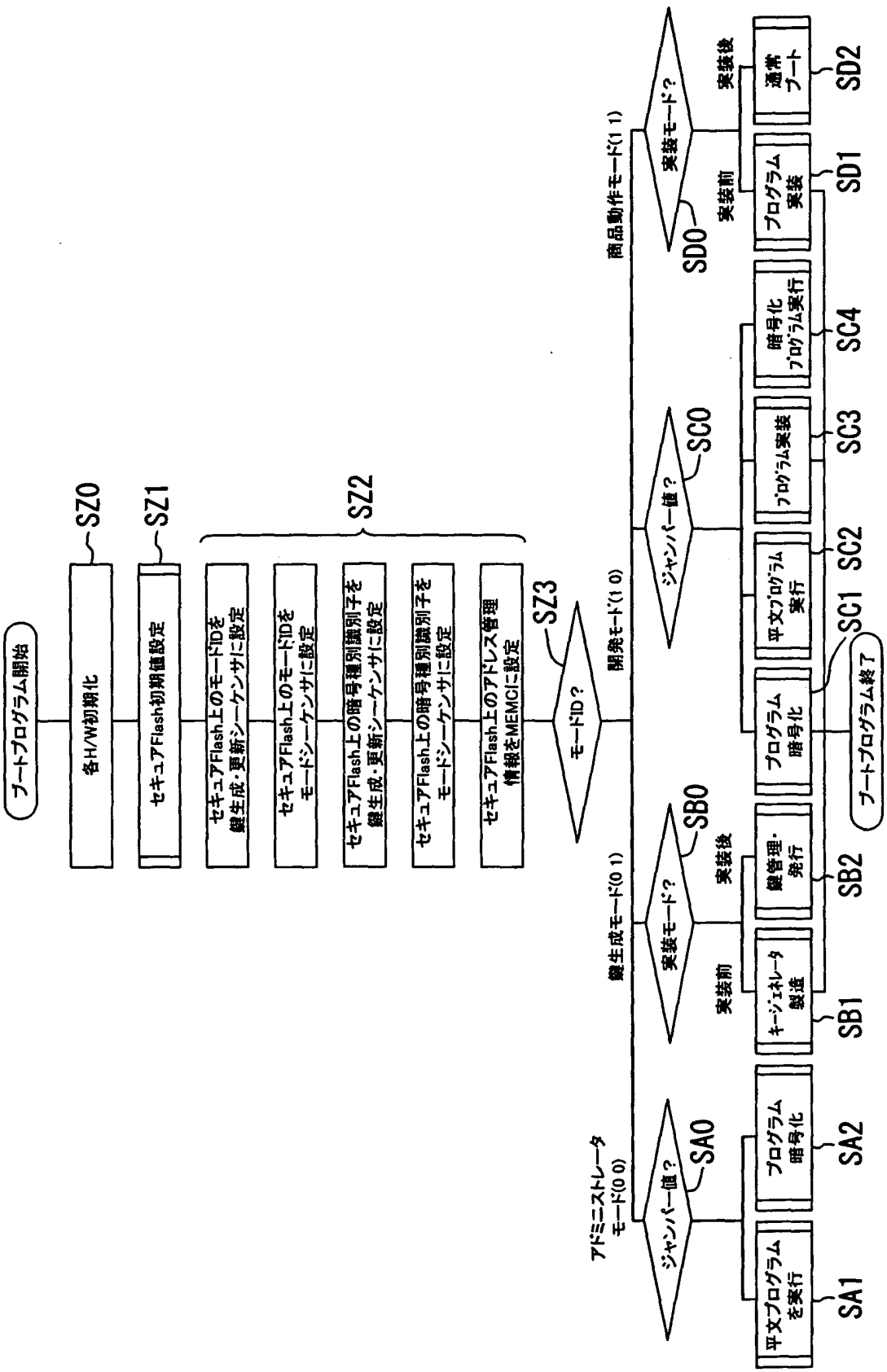
【図１】


DSP
100外部メモリ
101
外部Flash
102
外部RAM
外部ツール
110
120外部バス
1 セキュアLSI
外部入出力 モード制御
プログラム処理部
スルー部
プログラム復号用 暗号エンジン
プログラム固有鍵 格納レジスタ
データ処理部
スルー部
データ暗/復号用 暗号エンジン
データ用固有鍵 格納レジスタ
コマンド入出力部
内部RAM
ブートROM
モードID 格納レジスタ
暗号種別識別子 格納レジスタ
鍵生成・更新 シーケンサ
プログラム暗号鍵
ジャンパ
モードシーケンサ
モードID 格納レジスタ
暗号種別識別子 格納レジスタ
MEMC
入出力制御信号生成部
アドレス区分 格納レジスタ
外部アクセスアドレス 判定部
コモンバスアドレス格納部
秘密鍵演算処理部
種格納レジスタ
乱数格納レジスタ
固有ID格納レジスタ
暗号鍵格納レジスタ
CPU
クロック 改竄検出
アキュアクロック
HASH 演算
バッファ
生鍵格納レジスタ
コモンバス92
通信レジスタ
セキュアFlash アクセス制御
プライベートバス 91
セキュアFlash テスト制御
書き換え 不可領域 書込みフラグ
セキュアFlash
ジャンパ
50
54
51
52
53
55
56
58
31
60
40
41
42
43
80
84
81
83
82
35
30
32
2
65
70
20
95
44
10
14
13
12
11

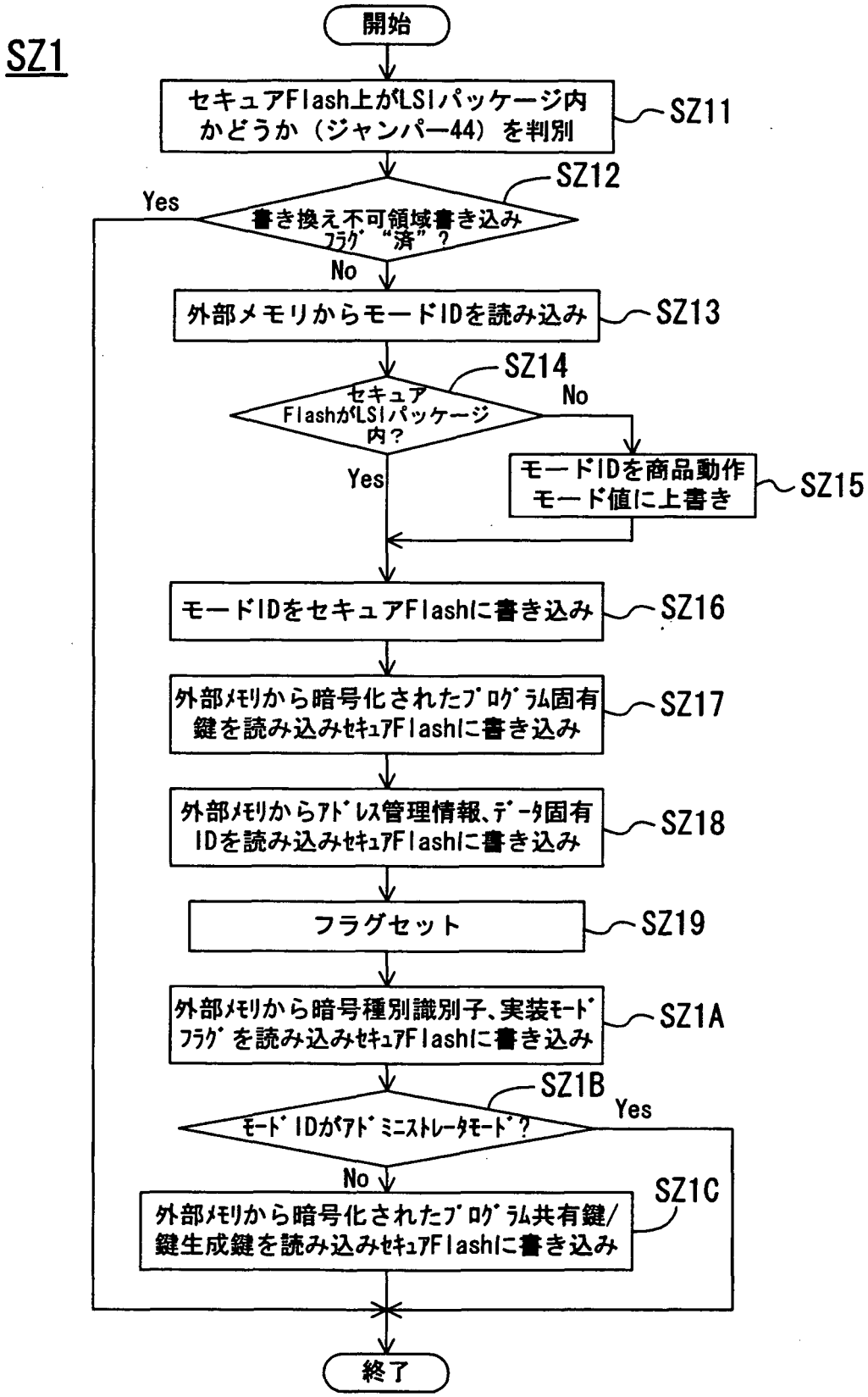
【図２】


<アドミニストレータモード'(0 0)>
PA0
初期値設定
管理者用LSI
PA1
雛生成プログラム開発
雛生成プログラム
PA2
雛生成プログラム暗号化
雛生成(任意)
・雛生成鍵で暗号化された雛生成プログラム
・暗号化雛生成鍵
・雛生成プログラムのHASH値
雛生成用LSI
PB0
初期値設定
PB1
キージェネレータ製造(雛生成プログラム実装)
PB2
雛管理・実行(雛生成プログラム実行)
プログラム固有鍵で暗号化された雛生成プログラム
暗号化プログラム共有鍵
暗号化プログラム固有鍵
データ固有ID 等
<雛生成モード'(0 1)>
モードID
暗号化プログラム固有鍵(当初は任意)
アドレス管理情報
データ固有ID(当初は任意)
暗号種別識別子
実装モードフラグ
暗号化雛生成鍵
モードID
暗号化プログラム固有鍵(任意)
アドレス管理情報
データ固有ID(任意)
暗号種別識別子
実装モードフラグ
<開発モード'(1 0)>
PC0
初期値設定
開発用LSI
PC1
アプリプログラム開発
アプリプログラム
PC2
アプリプログラム暗号化
・プログラム共有鍵で暗号化されたアプリプログラム
・暗号化共有鍵
・アプリプログラムのHASH値
PC3
アプリプログラム実装
PC4
アプリプログラムデバック
・プログラム固有鍵で暗号化されたアプリプログラム
モードID
暗号化プログラム固有鍵
アドレス管理情報
データ固有ID
暗号種別識別子
実装モードフラグ
暗号化プログラム共有鍵
<商品動作モード'(1 1)>
PD0
初期値設定
商品LSI
PD1
商品実装
・プログラム固有鍵で暗号化されたアプリプログラム
PD2
商品動作

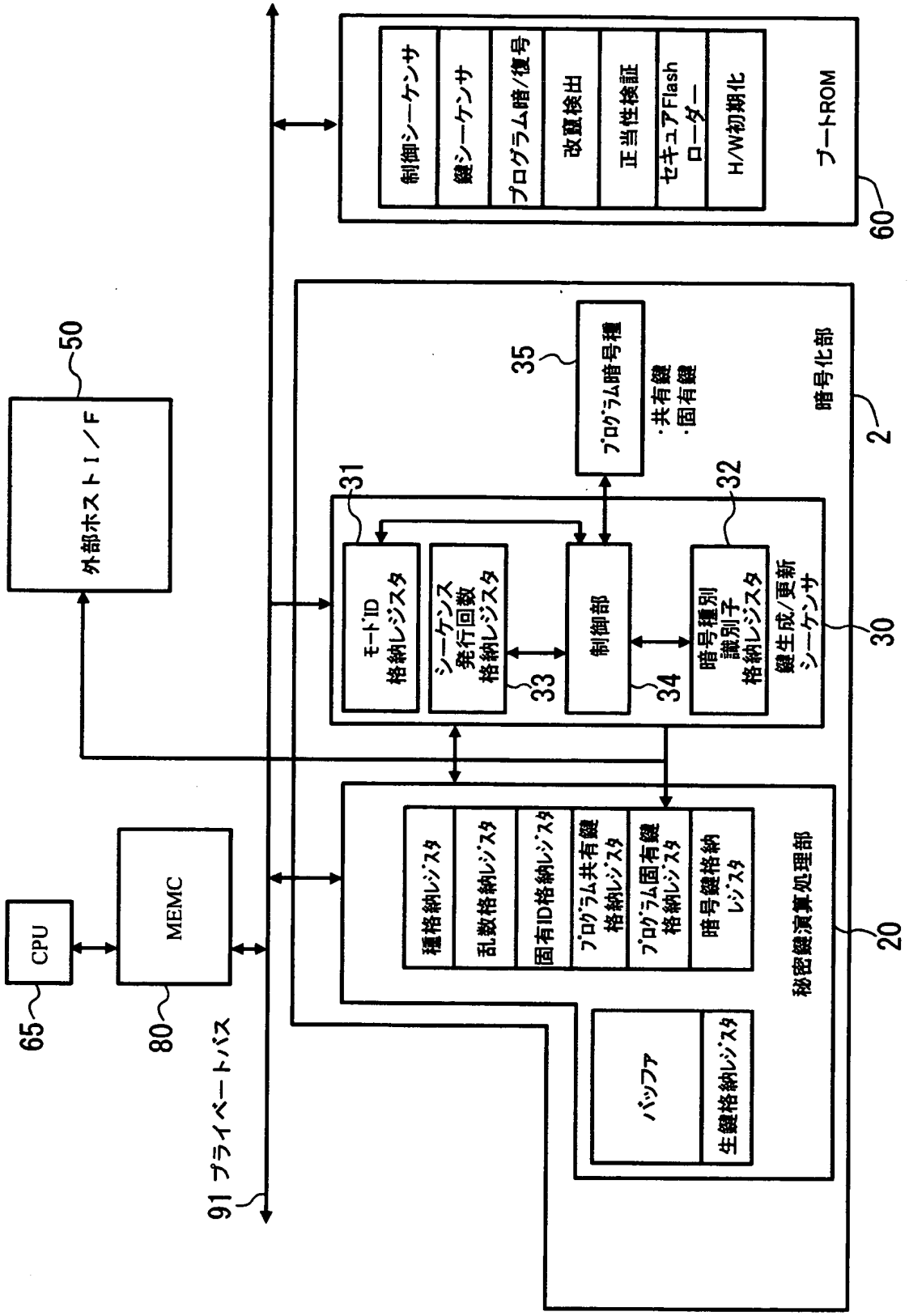
【図３】


ブートプログラム開始
各H/W初期化
SZ0
セキュアFlash初期値設定
SZ1
セキュアFlash上のモードIDを鍵生成・更新シーケンサに設定
セキュアFlash上のモードIDをモードシーケンサに設定
セキュアFlash上の暗号種別識別子を鍵生成・更新シーケンサに設定
セキュアFlash上の暗号種別識別子をモードシーケンサに設定
セキュアFlash上のアドレス管理情報をMEMCIに設定
SZ2
SZ3
モードID？
開発モード(1 0)
商品動作モード(1 1)
ジャンパー値？
SC0
実装モード？
SD0
実装前
実装後
プログラム実装
SD1
通常ブート
SD2
暗号化プログラム実行
SC4
プログラム実装
SC3
平文プログラム実行
SC2
プログラム暗号化
SC1
ブートプログラム終了
鍵生成モード(0 1)
実装モード？
SB0
実装前
実装後
鍵管理・発行
SB2
キージェネレータ製造
SB1
プログラム暗号化
SA2
アドミニストレータモード(0 0)
ジャンパー値？
SA0
平文プログラムを実行
SA1

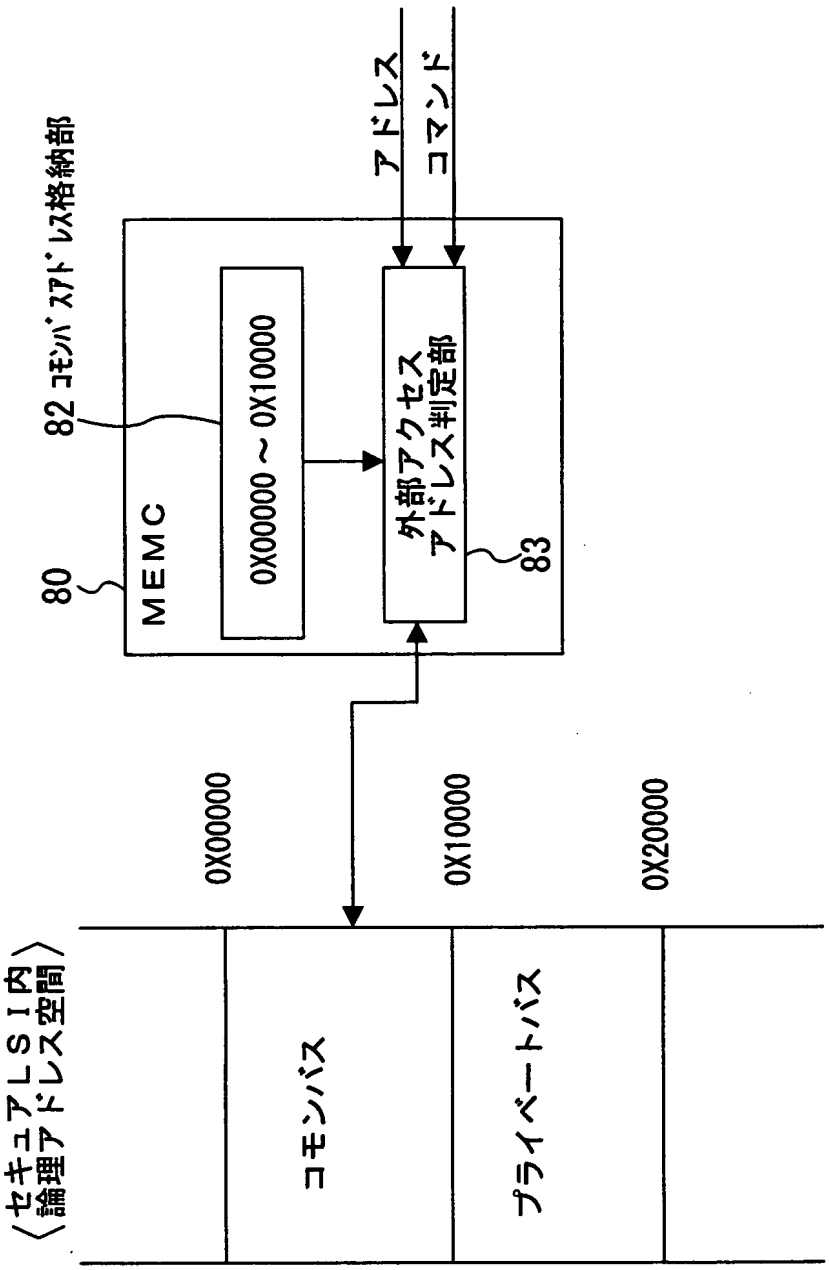
【図４】


SZ1
開始
セキュアFlash上がLSIパッケージ内かどうか（ジャンパー44）を判別
SZ11
書き換え不可領域書き込みﾌﾗｸﾞ“済”？
SZ12
Yes
No
外部メモリからモードIDを読み込み
SZ13
セキュアFlashがLSIパッケージ内？
SZ14
No
Yes
モードIDを商品動作モード値に上書き
SZ15
モードIDをセキュアFlashに書き込み
SZ16
外部ﾒﾓﾘから暗号化されたﾌﾟﾛｸﾞﾗﾑ固有鍵を読み込みｾｷｭｱFlashに書き込み
SZ17
外部ﾒﾓﾘからｱﾄﾞﾚｽ管理情報、ﾃﾞｰﾀ固有IDを読み込みｾｷｭｱFlashに書き込み
SZ18
フラグセット
SZ19
外部ﾒﾓﾘから暗号種別識別子、実装ﾓｰﾄﾞﾌﾗｸﾞを読み込みｾｷｭｱFlashに書き込み
SZ1A
ﾓｰﾄﾞIDがｱﾄﾞﾐﾆｽﾄﾚｰﾀﾓｰﾄﾞ？
SZ1B
Yes
No
外部ﾒﾓﾘから暗号化されたﾌﾟﾛｸﾞﾗﾑ共有鍵/鍵生成鍵を読み込みｾｷｭｱFlashに書き込み
SZ1C
終了

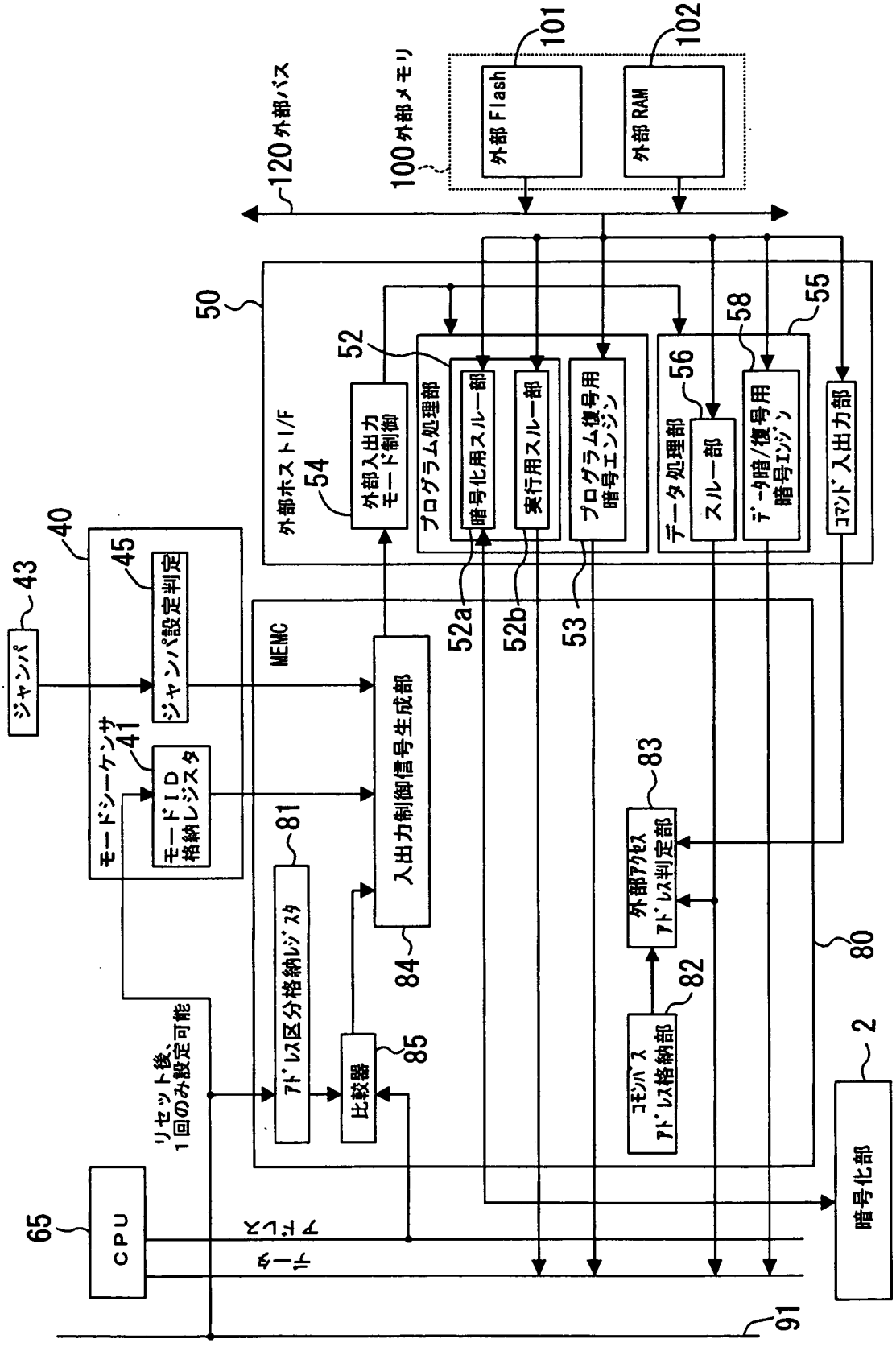
【図５】


制御シーケンサ
鍵シーケンサ
プログラム暗/復号
改竄検出
正当性検証
セキュアFlash ローダー
H/W初期化
ブートROM
60
暗号化部
2
35
プログラム暗号種
・共有鍵
・固有鍵
31
32
モードID 格納レジスタ
シーケンス 発行回数 格納レジスタ
制御部
暗号種別 識別子 格納レジスタ
鍵生成/更新 シーケンサ
30
33
34
外部ホストI／F
50
種格納レジスタ
乱数格納レジスタ
固有ID格納レジスタ
プログラム共有鍵 格納レジスタ
プログラム固有鍵 格納レジスタ
暗号鍵格納 レジスタ
秘密鍵演算処理部
20
バッファ
生鍵格納レジスタ
CPU
65
MEMC
80
91 プライベートバス

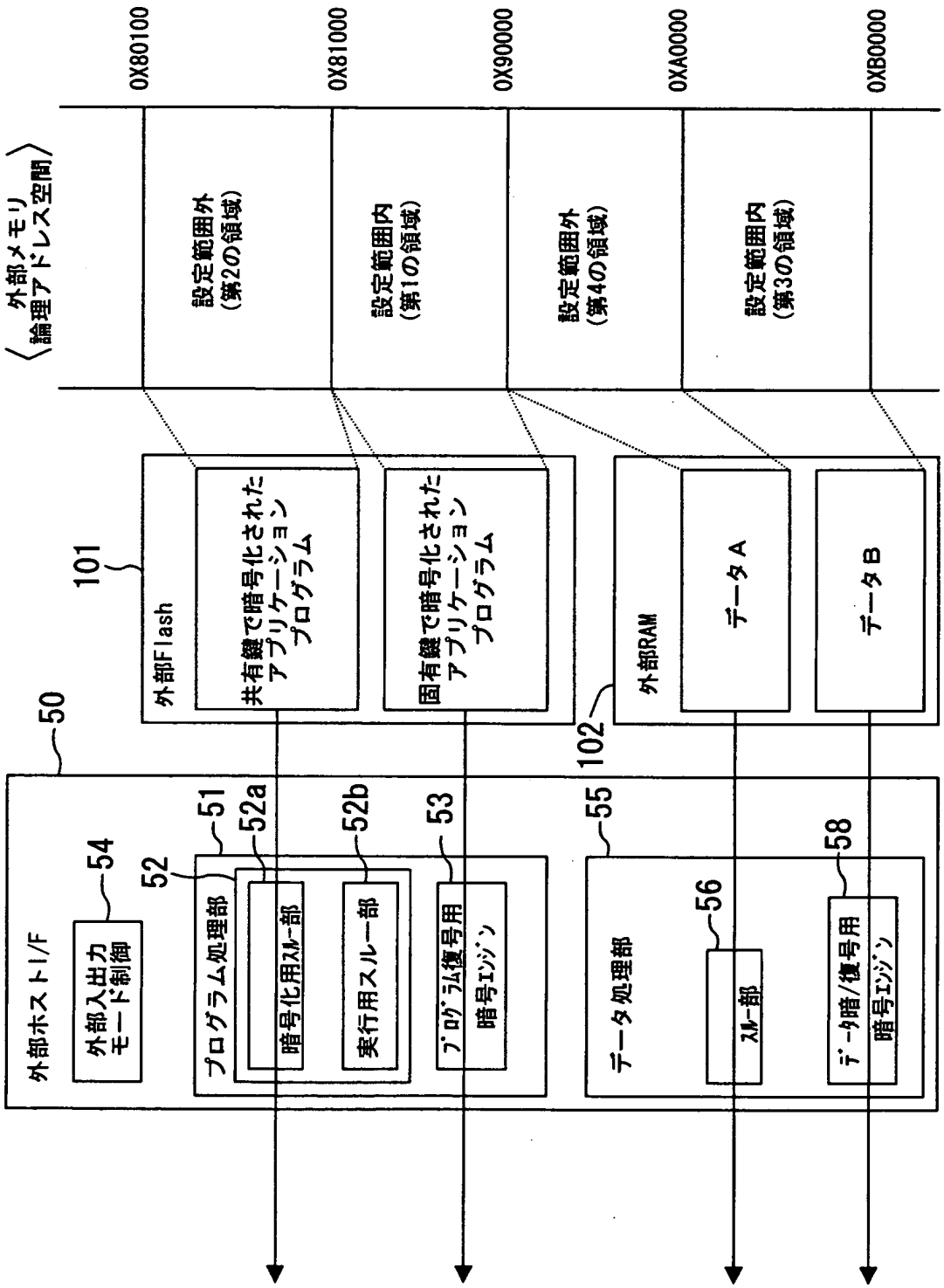
【図６】


〈セキュアＬＳＩ内
論理アドレス空間〉
0X00000
0X10000
0X20000
コモンバス
プライベートバス
80
MEMC
82 ｺﾓﾝﾊﾞｽｱﾄﾞﾚｽ格納部
0X00000 ～ 0X10000
外部アクセス
アドレス判定部
83
アドレス
コマンド

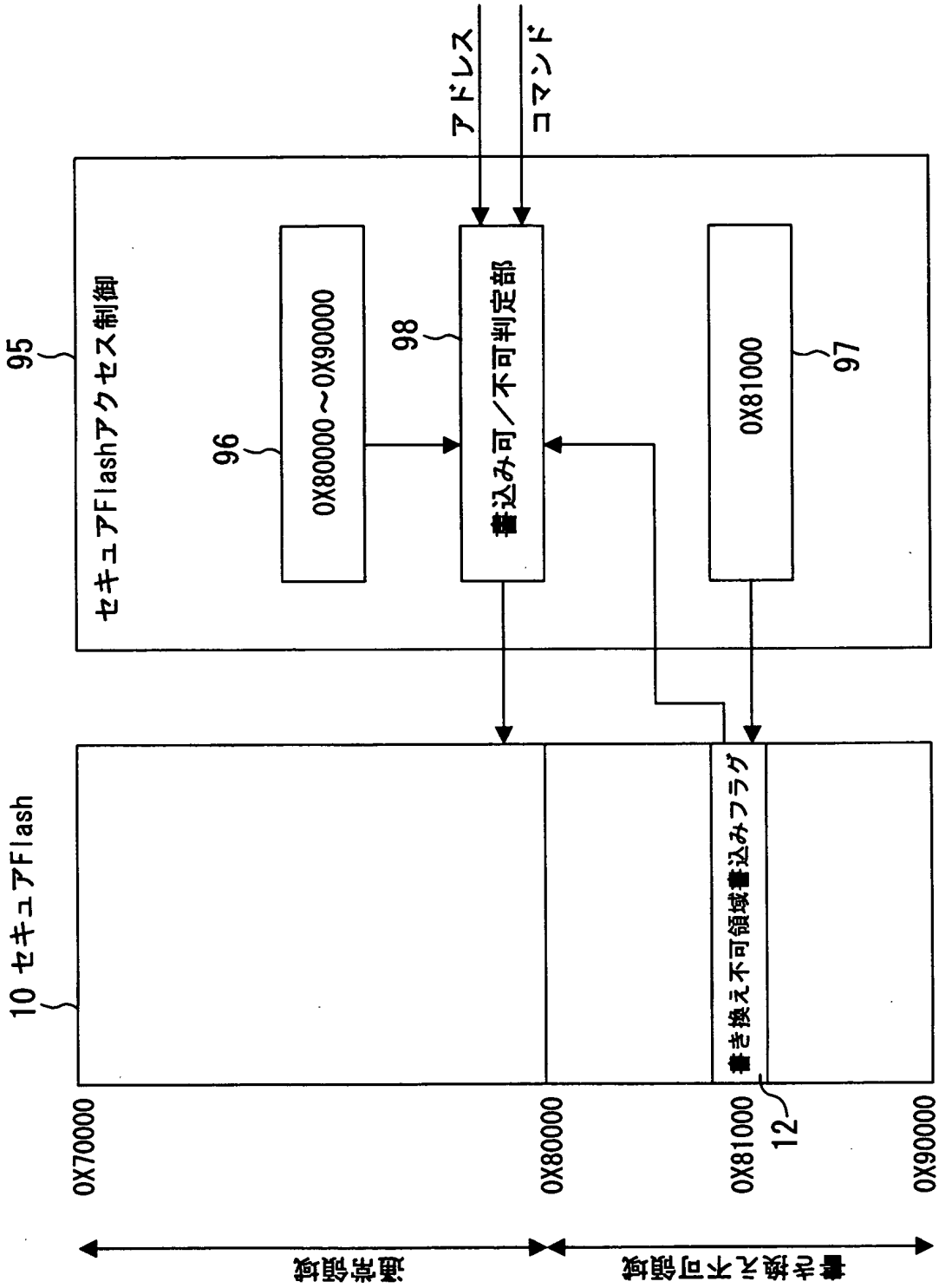
【図７】


100外部メモリ
101
外部Flash
102
外部RAM
120外部バス
50
外部ホストI/F
52
外部入出力モード制御
54
プログラム処理部
暗号化用スルー部
実行用スルー部
プログラム復号用暗号エンジン
データ処理部
56
スルー部
58
データ暗/復号用暗号エンジン
55
ｺﾏﾝﾄﾞ入出力部
52a
52b
53
40
45
ジャンパ設定判定
43
ジャンパ
モードシーケンサ
41
モードID格納レジスタ
MEMC
81
ｱﾄﾞﾚｽ区分格納ﾚｼﾞｽﾀ
入出力制御信号生成部
84
比較器
85
83
外部ｱｸｾｽｱﾄﾞﾚｽ判定部
82
ｺﾓﾝﾊﾞｽｱﾄﾞﾚｽ格納部
80
2
暗号化部
リセット後、1回のみ設定可能
65
CPU
ｱﾄﾞﾚｽ
ﾃﾞｰﾀ
91

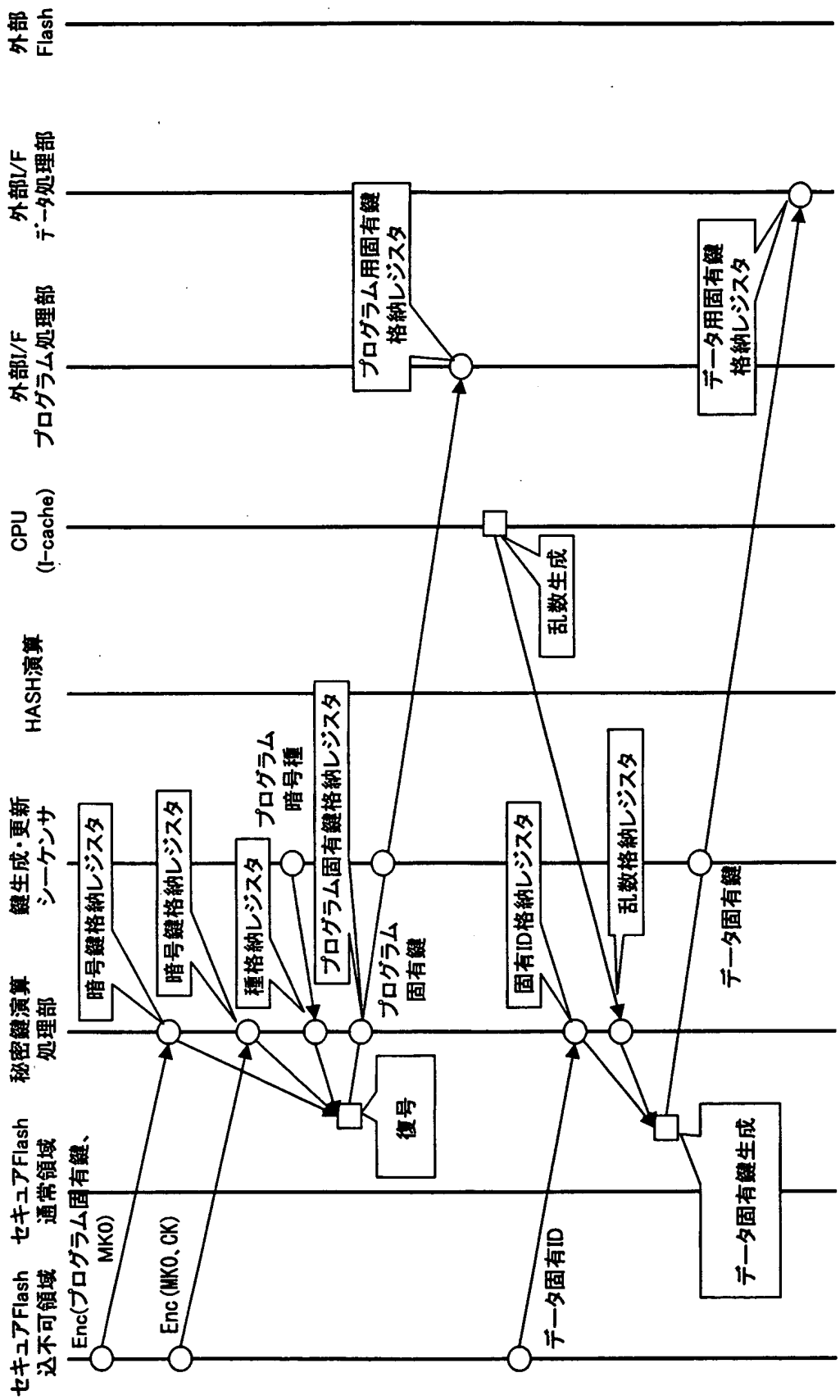
【図８】


〈外部メモリ論理アドレス空間〉
0X80100
0X81000
0X90000
0XA0000
0XB0000
設定範囲外（第2の領域）
設定範囲内（第1の領域）
設定範囲外（第4の領域）
設定範囲内（第3の領域）
101
外部Flash
共有鍵で暗号化されたアプリケーションプログラム
固有鍵で暗号化されたアプリケーションプログラム
102
外部RAM
データA
データB
50
外部ホストI/F
外部入出力モード制御
54
52
プログラム処理部
51
52a
暗号化用スルー部
52b
実行用スルー部
53
ﾌﾟﾛｸﾞﾗﾑ復号用暗号ｴﾝｼﾞﾝ
55
データ処理部
56
ｽﾙｰ部
58
ﾃﾞｰﾀ暗/復号用暗号ｴﾝｼﾞﾝ

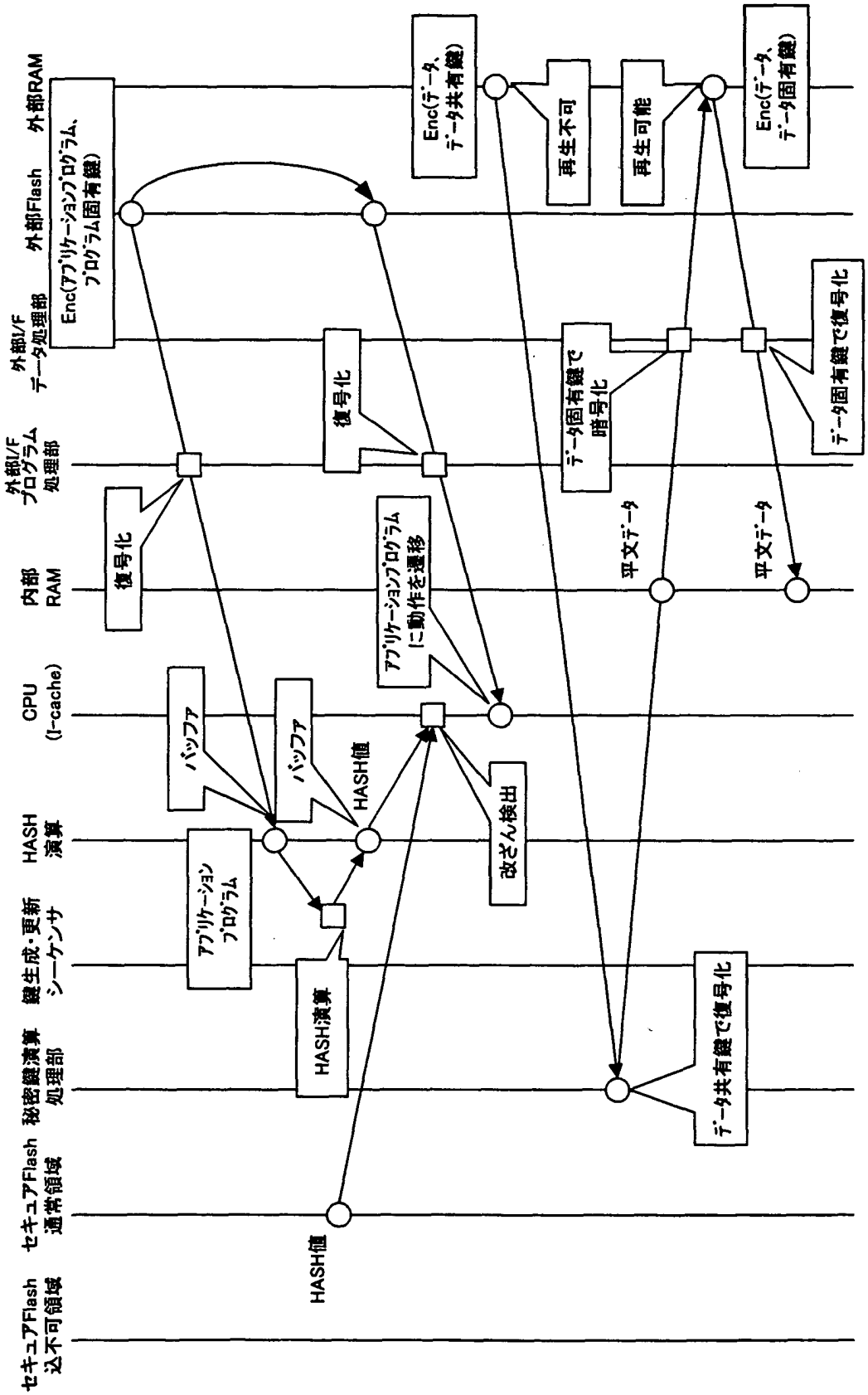
【図９】


アドレス
コマンド
95
セキュアFlashアクセス制御
96
0X80000～0X90000
98
書込み可／不可判定部
0X81000
97
10 セキュアFlash
書き換え不可領域書込みフラグ
0X70000
0X80000
0X81000
12
0X90000
通常領域
書き換え不可領域

【図１０】


セキュアFlash 込不可領域
セキュアFlash 通常領域
秘密鍵演算 処理部
鍵生成・更新 シーケンサ
HASH演算
CPU (I-cache)
外部I/F プログラム処理部
外部I/F データ処理部
外部 Flash
Enc(プログラム固有鍵、MK0)
Enc (MK0、CK)
暗号鍵格納レジスタ
暗号鍵格納レジスタ
種格納レジスタ
プログラム 暗号種
プログラム固有鍵格納レジスタ
プログラム 固有鍵
復号
プログラム用固有鍵 格納レジスタ
乱数生成
固有ID格納レジスタ
乱数格納レジスタ
データ固有ID
データ固有鍵
データ固有鍵生成
データ用固有鍵 格納レジスタ

【図１１】


セキュアFlash 込不可領域
セキュアFlash 通常領域
秘密鍵演算 処理部
鍵生成・更新 シーケンサ
HASH 演算
CPU (I-cache)
内部 RAM
外部I/F プログラム 処理部
外部I/F データ処理部
外部Flash
外部RAM
Enc(アプリケーションプログラム、プログラム固有鍵)
Enc(データ、データ共有鍵)
再生不可
再生可能
Enc(データ、データ固有鍵)
復号化
復号化
データ固有鍵で暗号化
データ固有鍵で復号化
アプリケーションに動作を遷移
平文データ
平文データ
バッファ
バッファ
HASH値
改ざん検出
アプリケーションプログラム
HASH演算
データ共有鍵で復号化
HASH値

【書類名】　要約書

【要約】

【課題】　セキュリティレベルの高い半導体装置を提供する。

【解決手段】　セキュアＬＳＩ１は、プログラムの暗号化を行う暗号化部２と、外部メモリ１００との間でプログラムやデータの入出力を行うための外部Ｉ／Ｆ５０とを備えている。暗号化部２において、鍵生成・更新シーケンサ３０が、実行が許されないと判断したシーケンスについて、秘密鍵演算処理部２０の動作を禁止する。外部Ｉ／Ｆ５０では、プログラム処理部５１とデータ処理部５５とが別個独立に構成されている。

【選択図】　図１

出 願 人 履 歴 情 報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社